# 密钥管理

2020年8月25日 17:36

1. 对称密码体制密钥分级
    a. 初级密钥：真正用于加解密数据的密钥，由系统产生或用户提供。初级通信密钥和初级绘画密钥生存周期很短，一般存储在工作存储器；初级文件密钥生存周期和所保护的文件一样长，一般以密文形式存储
    b. 二级密钥：用于保护初级密钥的密钥，由系统产生或专职密钥安装人员提供。生存周期一般较长，可以在专用装置明文存储或以密文形式存储
    c. 主密钥：对二级密钥进行保护的密钥，是密钥管理方案中的最高级密钥。由密钥专职人员随即产生并妥善安装，生存周期很长。由于只能明文存储，需要存储在高度安全的专用装置
2. 公钥密码体制一般以证书形式交给PKI管理
    a. 数字证书：主要包含主体身份、主体公钥、CA名、CA签名